COPY

State of Rhode Island
Complaint to Search and Seize Property / or Person

TO Neal Usdin Justice of the Supreme, Superior Court, or Judge of the District Court of the State of Rhode Island.

a) **Detective Corporal Stephen Evans**, of the East Providence Police Department and a member of the Rhode Island Internet Crimes Against Children Task Force.

b) _____ a person authorized by law to bring complaints for violation of the law which it is my responsibility to enforce/a person who has a right to possession of the property stolen, embezzled, or obtained by false pretense or pretenses:

ON OATH COMPLAINS THAT:

(1) Certain property has been stolen or embezzled, or obtained by false pretenses, or pretenses, with intent to cheat or defraud within this state or elsewhere.

(2) Certain property has been kept, suffered to be kept, concealed, deposited, or possessed in violation of law, or for the purpose of violating the law;

(3) Certain property is designed or intended for use, or is or has been used in violation of law, or as a means of committing a violation of law;

(4) Certain property contains evidence of a crime;

and requests that a warrant to search for and seize said property/person be issued and if the same be subject to forfeiture, that the property be forfeited.

The person/property or articles to be searched for and/or seized is described as follows: **Computer hardware, computer software, mobile devices, and portable digital storage devices, to include the contents therein. Additionally, any and all computer-related documentation, records, documents, material, proceeds, and passwords or other data security devices related to the possession and transfer of child pornography. Refer to Attachments "A" and "B" attached hereto and made a part hereof.**

The name of the owner or keeper, thereof (if known) is: **Unknown.**

The place or person to be searched is described as follows: **The premises located at 538 Broadway, Providence, Rhode Island 02909. Said premises is described as a stone church with "St. Mary's Catholic Parish" affixed to a sign in the front of the building. The search will include exterior buildings on the property to include the detached yellow building commonly known as the rectory. The search will include storage spaces located on the premises used by residents.**

Subscribed and sworn to before me:

10/21/21
Date

Judge/Justice

Complainant

Search Warrant

State Ex rel	Member of the East Providence Police Department and a Rhode Island Internet Crimes Against Children Taskforce Member: **Detective Corporal Stephen Evans**	County: **Providence**
vs. Respondent: **St. Mary's Church of Providence 538 Broadway, Providence, Rhode Island 02909**		To: An Officer authorized by law to execute the within warrant,

Complaint and affidavit having been made to me under oath by **Detective Corporal Stephen Evans** and as I am satisfied that there is probable cause for the belief therein set forth that grounds for issuing a search warrant exist, you are hereby commanded diligently to search the place or person herein described for the property specified and to bring such property or articles, and to summon the owner, or keeper thereof, if any be named in the complaint, if to be found by you, to appear before the 6th District Court in the district where such property shall have been seized, namely the Sixth Division of the District Court of Rhode Island.

Place or person to be searched: **The premises located at 538 Broadway, Providence, Rhode Island 02909. Said premises is described as a stone church with "St. Mary's Catholic Parish" affixed to a sign in the front of the building. The search will include exterior buildings on the property to include the detached yellow building commonly known as the rectory. The search will include storage spaces located on the premises used by residents.**

Property or articles to be searched for: **Computer hardware, computer software, mobile devices, and portable digital storage devices, to include the contents therein. Additionally, any and all computer-related documentation, records, documents, material, proceeds, and passwords or other data security devices related to the possession and transfer of child pornography. Refer to Attachments "A" and "B" attached hereto and made a part hereof.**

Name of owner, or keeper, thereof if known to complainant: **Unknown.**

Said warrant shall be served in the daytime -- may be served in the nighttime -- within seven (7) days from the issuance hereof, AND IF NOT SERVED WITHIN SAID TIME TO BE RETURNED FORTHWITH TO A JUDGE SITTING IN THE ABOVE-NAMED COURT.

Property seized by you hereunder shall be safely kept by you under the direction of the Court so long as may be necessary for the purpose of being used as evidence in any case. As soon as may be thereafter, if the same be subject to forfeiture, such further proceedings shall be had thereon for forfeiture as is prescribed by law.

Hereof fail not and MAKE TRUE RETURN PROMPTLY OF THIS WARRANT TO A JUDGE THERE SITTING with your doings thereon, accompanied by a written inventory of any property taken to a judge sitting in the above-named court.

Issued at **Providence** in the county of **Providence** this 31 day of **October**, A.D. **2021**

Judge of the District Court
Justice of the Supreme/Superior Court

ACKNOWLEDGMENT OF RETURN

Warrant received on the _____ day of _____, 2021, from **Detective Corporal Stephen Evans – ICAC Taskforce** at **Providence**.

Clerk

AFFIDAVIT

Your affiant, Detective Corporal Stephen Evans, on oath does depose and state that I am a sworn member of the East Providence Police Department and have been continuously employed in that capacity for over ten (10) years. I am currently assigned to the Rhode Island Internet Crimes Against Children (ICAC) Task Force, and as such am engaged in the investigation of acts committed in violation of the General Laws of the State of Rhode Island. The Rhode Island ICAC Task Force Program is administered by the Rhode Island State Police and supports a national network of multi-agency, multi-jurisdictional task forces engaged in investigations, forensic examinations, and prosecutions related to Internet crimes against children and technology-facilitated child sexual exploitation.

Your affiant knows that peer-to-peer networks are designed to facilitate the sharing of electronic files between participating members over the Internet. To become a member of a peer-to-peer network, a computer user installs file-sharing software on a computer which creates a "sharing folder", into which may be placed any electronic files available for other members on the network to copy. The user also gains the ability to copy any electronic files into his/her "sharing folder" from other network members. A single peer-to-peer network may consist of thousands of interconnected computers, and the electronic files available on that network are all stored on the individual members' computers rather than on a central host computer.

Your affiant knows from training that individuals seeking to obtain and share child pornographic movies, images and materials frequently use file-sharing programs. When file-sharing programs are installed on a computer they allow the user, known as a peer, to search the network for pictures, movies, and other digital files by entering a text-based search term. When a member of a peer-to-peer network submits a request for a particular electronic file (such as "PTHC", which stands for "pre-teen hard core"), the network program provides the following: a list of available electronic files that contain the initial search term; the hash value for each available electronic file; and the Internet Protocol (IP) address of the computer that is sharing the file that is being requested (see detailed explanations of the terms hash value and IP address directly below). The listed electronic files may then be copied from the peer-to-peer network to the requesting member's computer. Using peer-to-peer software, a user requesting the download of a specific file from the returned list connects to the peer-to-peer networked computer offering that file.

Peer-to-peer file-sharing networks identify the IP address associated with the computer sharing a file(s) on the network. An IP address is a unique routing number associated with a computer connected to the Internet which

functions in the routing of data between source and destination. IP addresses are owned by Internet service providers (such as Verizon, Cox Communications and Comcast) who, in turn, assign them to customers for Internet access. An IP address is represented by numbers separated by periods (such as 123.98.332.401), or numbers and letters separated by colons (such as 1234:abcd:12ad:34cd:dcba:4321:1a2b:3c4d), which identifies that computer connected on the Internet at a given date and time. Normally, IP address assignments by Internet service providers are unique in that no two computers logged onto the Internet at the same date and time are assigned the same IP address. Internet service providers maintain records of the assignment of IP addresses to their individual subscribers.

Your affiant knows that peer-to-peer networks use hash values to verify the content of electronic files that are available for copying. A hash value is an alpha-numeric string (such as 2D92735A6DE77B49E6923D7B3F6EB78364C4C981) that is calculated by applying a mathematical algorithm to the electronic data that is contained in an electronic file. Only identical electronic files will have the same hash value and any change to the contents of an electronic file, no matter how slight, will result in a change to that file's hash value. Thus, hash values are commonly referred to as electronic fingerprints. Your affiant knows, through training, that over time numerous files have been identified through their specific hash values as confirmed child pornography. Identification has been made through the combined knowledge of law enforcement members throughout the United States, members of the National Center for Missing and Exploited Children (NCMEC), as well as members of the Internet Crimes Against Children (ICAC) Task Forces across the country.

Your affiant observed that a computer or other device using Internet Protocol (IP) address 72.82.21.56 was on a peer-to-peer file-sharing network on September 4, 2021 at 11:11:56 (UTC). A device connected to this IP address was sharing files of suspected child pornography. A single source direct connection was made to the aforementioned IP address and 71 files of suspected child pornography were downloaded.

Your affiant viewed a portion of the aforementioned files and confirmed several of the video files content to be consistent with the definition of child pornography as defined in Rhode Island General Law 11-9-1.3. One of the files is described below, and it will remain in the custody of the Rhode Island Internet Crimes Against Children Task Force. The video files are available for viewing for prosecutorial purposes.

File Name: Wanted Dad And Daughter-1
Description: This video is two minutes, and thirty-two seconds of a nude prepubescent female performing oral sex on an adult male.

Your affiant conducted an inquiry with the American Registry of Internet Numbers (ARIN) and determined that the owner of IP address 72.82.21.56 is Verizon Fios, 180 Washington Valley Road, Bedminster, NJ, 07921. The IP address was geolocated to the Providence area of Rhode Island. Geolocation is the process of approximating the location of a computer or other device connected to the internet based on its IP address. Your affiant sent legal process to Verizon for the subscriber of 72.82.21.56 on September 4, 2021 at 11:11:59 (UTC). Verizon responded to the legal process and identified the subscriber as St. Mary's Church of Providence, 538 Broadway, Floor 1, Providence, Rhode Island 02909. The legal process identified a contact customer name of Claire Gruneberg. An open-source search revealed Claire Gruneberg is employed as a bookkeeper for St. Mary's Church. Additionally, your affiant is aware that bookkeepers are commonly listed as subscribers for commercial properties because they are responsible for bill payment.

Your affiant is aware through training and experience, that multiple individuals often share the internet signal within the same building. Your affiant is also aware that a traditional Wi-Fi router can broadcast an internet signal up to 150 feet, which allows all members, within close proximity of a building, access to the same internet signal. Additionally, your affiant is aware that each member within close proximity of a building have equal access to the internet connection and it is not possible to discern who is utilizing the internet for illicit purposes without reviewing all digital media within the building. Therefore, your affiant reasonably believes that occupants in multiple buildings have equal access to the internet connection at 538 Broadway, Providence, Rhode Island 02909.

During the month of October 2021, your affiant responded to the area of 538 Broadway, Providence, Rhode Island 02909. Your affiant observed the building to be a stone Church with a St. Mary's Catholic Parish sign in the front of the building. Your affiant observed a yellow building, next to the church, with a "Church of St. Mary" sign in front. This building houses the church offices and rectory. Your affiant conducted a check of the publicly available Wi-Fi signals while standing in close proximity to St. Mary's Parish and located one Service Set Identified (SSID) identified as St. Mary's Church _Ext. This Wi-Fi signal was locked meaning only those with the password can utilize this Wi-Fi signal. Additionally, your affiant is aware that the SSID is the name of a wireless network, also known as Network ID. This is viewable to anyone with a wireless device within reachable distance of the network. Your affiant conducted a check of open-source law enforcement databases and determined that 538 Broadway, Providence, Rhode Island is owned by St. Mary's Church. Furthermore, your affiant contacted St. Mary's Church and spoke with Claire Gruneberg who advised your affiant that the Church mailing address was 538 Broadway, Providence, Rhode Island 02909.

When a user is connected to a peer-to-peer file sharing network, and is transferring child pornography, the Internet Crimes Against Children Task Force (ICAC) is notified. Your affiant observed a computer or other device using Internet Protocol (IP) address 72.82.21.56 was on a peer-to-peer file-sharing network on Sunday, September 26, 2021 at 5:32PM, Friday October 15, 2021 at 3:12PM, and Sunday, October 17, 2021 3:58PM. The connection on October 15, 2021, revealed nine additional files of child pornography. Your affiant viewed a portion of the aforementioned files and confirmed several of the video files content to be consistent with the definition of child pornography as defined in Rhode Island General Law 11-9-1.3. One of the files is described below, and it will remain in the custody of the Rhode Island Internet Crimes Against Children Task Force. The video files are available for viewing for prosecutorial purposes.

File Name: 000007.mp4
Description: This video is thirty-three minutes and thirteen seconds long. The video is of a nude pubescent female showing her hands being bound behind her back by an individual in a black robe covering the face and extremities. The robed individual forces the prepubescent female to perform oral sex on an artificial object shaped like an adult male penis. The robed individual then places the object in the vagina of the pubescent female.

Your affiant researched events and activities that take place at St. Mary's Church. Your affiant compared these times to the connection times that were observed. It appears that the peer-to-peer connections take place during the off-hours of church activities.

Your affiant is aware through experience, education and training that those who have demonstrated an interest or preference in sexual activity with children or in sexually explicit visual images depicting children are likely to keep secreted, but readily at hand, sexually explicit visual images depicting children. In some instances, the suspect keeps these depictions as a means of plying, broaching, or titillating the sexual interests of new child victims or otherwise lowering the inhibitions of other potential child sexual partners by showing them that other children participate in this kind of activity. Still, in other instances, the depictions are a means of arousing the suspect.

These depictions tend to be extremely important to such individuals and are likely to remain in the possession of or under the control of such an individual for extensive time periods, perhaps for a lifetime. Those who actively engage in such illegal activity (possession and dissemination of child pornography) with the use of computers can also hide, encrypt, compress, uniquely modify and/or erase, or attempt to erase, some of their computer files, programs, code, directories, folders and disks. Your affiant knows through training and

experience that even if a computer file or image is purposefully deleted, that data can often be recovered through forensic analysis. Additionally, your affiant knows through training and experience that these individuals can keep digital media on their person due to the relatively small size of the media. Those who actively engage in such illegal activity are also known to hide such media in storage spaces within and around their property, including detached garages, sheds, basements, and other similar storage locations, in an attempt to hide such contraband from other residents, guests and members of law enforcement.

Therefore, your affiant reasonably believes that the Internet connection at 538 Broadway, Providence, Rhode Island 02909, was used by mobile devices, computer hardware, and/or computer software on September 4, 2021 and October 15, 2021, to facilitate the possession and offering of files that contain child pornography. Based on the aforementioned information, your affiant requests that a search warrant be issued for the premises located at 538 Broadway, Providence, Rhode Island 02909, in order to search and seize any and all mobile devices, computer hardware, computer software, to include the contents therein. The search will also include computer-related documentation, records, documents, material, and passwords or other data security devices related to the acquisition, possession and transfer of child pornography. The search will include storage spaces located on the premises used by the residents. Refer to Attachment "A" attached hereto and made a part hereof.

Your affiant requests that a member of the Rhode Island State Police Computer Crimes Unit and/or qualified designee be allowed to conduct an on-site forensic preview of the seized electronic media for evidence related to the possession and transfer of child pornography. Furthermore, your affiant requests that a member of the Rhode Island State Police Computer Crimes Unit and/or qualified designee be allowed to conduct an off-site forensic analysis and search on the seized evidence; this request is due to the complex nature of computer forensics as noted in Attachment "B" which is attached hereto and made a part hereof.

_____ _____

Date Affiant

Providence Sc. In **Providence** this _____ day of **October, 2021**
before me personally came **Detective Corporal Stephen Evans** and made oath to the truth of the foregoing.

_____

Judge of the District Court
Justice of the Supreme/Superior Court

RETURN OF SERVICE

STATE OF RHODE ISLAND AND PROVIDENCE PLANTATIONS KENT, SC.

At **538 Broadway, Providence, Rhode Island** _____, pursuant to the within warrant I have made search during the –**DAYTIME**-- as commanded and submit herewith a written inventory of property taken :

See attached evidence recovery log

I have also given to _____, from whose premises said property was taken -- a copy of the within warrant -- I have left a copy of the within warrant at 538 Broadway, Providence, Rhode Island on the place from which said property was taken -- but I did not find the person from whose premises said property was taken but left a copy of said warrant -- on the place from which the property was taken.

_____

Authorized Officer

ATTACHMENT "A"

The following terms and definitions are provided in support of the application to search for and seize evidence:

Computer Hardware refers to the physical components of a computer system. Computer hardware can also be installed inside, or connected to the outside, of a computer system. Hardware includes, but is not limited to, desktop computers, laptop computers, mobile devices, video gaming consoles, digital storage devices, digital cameras, and peripheral devices. Mobile devices include, but are not limited to, cell phones, smart phones, portable MP3 players, tablets, and e-reader devices. Digital storage devices include, but are not limited to, internal and external hard drives, USB flash drives, compact discs (CDs), digital video discs (DVDs), and Blu-ray discs. Peripheral devices include, but are not limited to, keyboards, printers, scanners, video display monitors (to include televisions being used as a display monitor), optical readers, and related communications devices – such as modems, wireless cards, GPS devices, cables, routers, switches and gateways.

Computer Software is digital code and files, which can be interpreted by a computer system. Software is stored in electronic, binary, magnetic, optical, transient, volatile, or any other digital form. Computer software includes, but is not limited to, operating systems, applications like word-processing, graphics, or spreadsheet programs, file sharing programs, utilities, compilers, interpreters, and communications programs such as email.

Computer-related Documentation consists of written, recorded, printed or electronically stored material(s), which explains or illustrates how to configure, access, control, operate, or interact with or use computer hardware, computer software, or other related items.

Records, Documents, and Materials include all items believed to be of evidentiary nature or evidence in any form including, but not limited to: printed "hard" copy records, phone records, written documents and their drafts or modifications, business and accounting records, books and ledgers, correspondence and notes; electronic records such as electronic text, electronic mail, text messages, website data and records, internet browser history, user activity data, digital images and digital video, photographs, drawings, internet accounts, peer-to-peer materials, live processes and services, network logs and records, audio recordings, records which reflect the ownership or control of computer hardware, computer software, records, documents, materials, and/or passwords or other data security devices, and documentation related to the identification of persons or entities which have control and possession of the place to be searched.

Passwords and other Data Security Devices consists of passwords, encryption keys, hardware devices, authentication devices, software programs, and biometric devices designed to effectuate authentication and/or hide, disguise, and prevent viewing or otherwise limit access to data and written records or notes.

ATTACHMENT "B"

Computer hardware, computer software, records, documents and materials, computer related documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits or contain evidence of a crime and/or (2) the objects may have been used to collect and store information about crimes in the form of electronic data.

Based upon your affiant's knowledge, training and experience, as well as on consultations with law enforcement officers in the area of computer forensics and investigations, it is known that searching and seizing information from computers often requires agents to seize most or all electronic storage devices, along with related peripherals, to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

Volume of Evidence. Computer storage devices, like hard drives, thumb drives, discs and mobile devices, can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she may store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of a crime. This sorting process may take weeks or months depending on the volume of data stored and it would be impractical to attempt this kind of data search on site.

Technical Requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, making it difficult to know before a search which expert is qualified to analyze the system and its data. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected or encrypted files. Evidence contained on computers/mobile devices/storage devices is extremely vulnerable to inadvertent or intentional modification or destruction, both from external sources or from destructive code imbedded in the system necessitating a controlled environment for complete and accurate analysis. Additionally, the nature of computer forensics is extremely time consuming process which can take weeks or months.

Searching computerized information for evidence or instrumentalities of crime commonly requires seizure of most or all of a computer system's input/output peripheral devices, related software, documentation and data security devices, including passwords, so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

The peripheral devices, which allow users to enter or retrieve data from the storage devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (I/O) devices in order to read the data on the system. It is important that the analysts be able to properly reconfigure the system as it now operates in order to accurately retrieve the evidence listed above. Additionally, the analyst needs the relevant system software - operating systems, interfaces and hardware drivers, any application software which may have been

used to create the data, whether stored on hard drives or external media, as well as related instruction manuals or other documentation and data security devices.